Critical Updates to NIST's CUI Publications: What You Need to Know

January 10, 2024 || 1:00 PM -2:00 PM Eastern

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Ron Ross
ron.ross@nist.gov

Victoria Yan Pillitteri
victoria.yan@nist.gov

Etiquette & Reminders

All participant microphones and cameras are **automatically muted**.

Please enter questions and comments for presenters in the WebEx Q&A.

Do not send questions via direct message to the host/panelists or in the chat feature.

Q&A and chat are NOT moderated.

Please be kind and courteous to one another.

For technical issues with WebEx, send a **PRIVATE chat/message via WebEx** to the Panelist ”WEBEX Help” or email: 800-171comments@list.nist.gov

FAQ

Will this webinar be recorded?

Yes. The event will be recorded and posted at the event site within 10 business days.

When will slides be posted?

The slides will be posted by close of business on **January 11, 2023** on the event site**.**

Does NIST issue CE/CPE credits?

No. NIST does not provide specific information regarding CE/CPE credits. Attendees are welcome to use their registration confirmation email to self-report to their certification bodies.

Where is the event site?

https://csrc.nist.gov/Events/2024/critical-updates-to-nist-cui-publications

Critical Updates to NIST's CUI Publications: What You Need to Know

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Ron Ross
ron.ross@nist.gov

Victoria Yan Pillitteri
victoria.yan@nist.gov

Agenda

https://csrc.nist.gov/projects/protecting-CUI

NIST SPECIAL PUBLICATION
SP 800-171
171
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

NIST Special Publication (SP) 800-171 at a Glance

Change Overview: Final Public Draft SP 800-171 Revision 3 and Initial Public Draft SP 800-171A Revision 3

Looking Ahead for the CUI Series

Contact Information and Q&A

SP 800-171 at a Glance

SECURITY REQUIREMENTS
FOR PROTECTING THE CONFIDENTIALITY OF CUI

NONFEDERAL
SYSTEMS & ORGANIZATIONS

PROCESSING, STORING, OR TRANSMITTING
CUI

DRAFT REV 3
SECURITY REQUIREMENTS & ASSESSMENT PROCEDURES AVAILBLE FOR COMMENT

INTERNATIONAL
USE & IMPACT

NEW & IMPROVED
SUPPLEMENTAL RESOURCES

ASSESSMENT PROCEDURES
SP 800-171A

ENHANCED SECURITY REQUIREMENTS
SP 800-172

ASSESSMENT PROCEDURES FOR ENHANCED SECURITY REQUIREMENTS
SP 800-172A

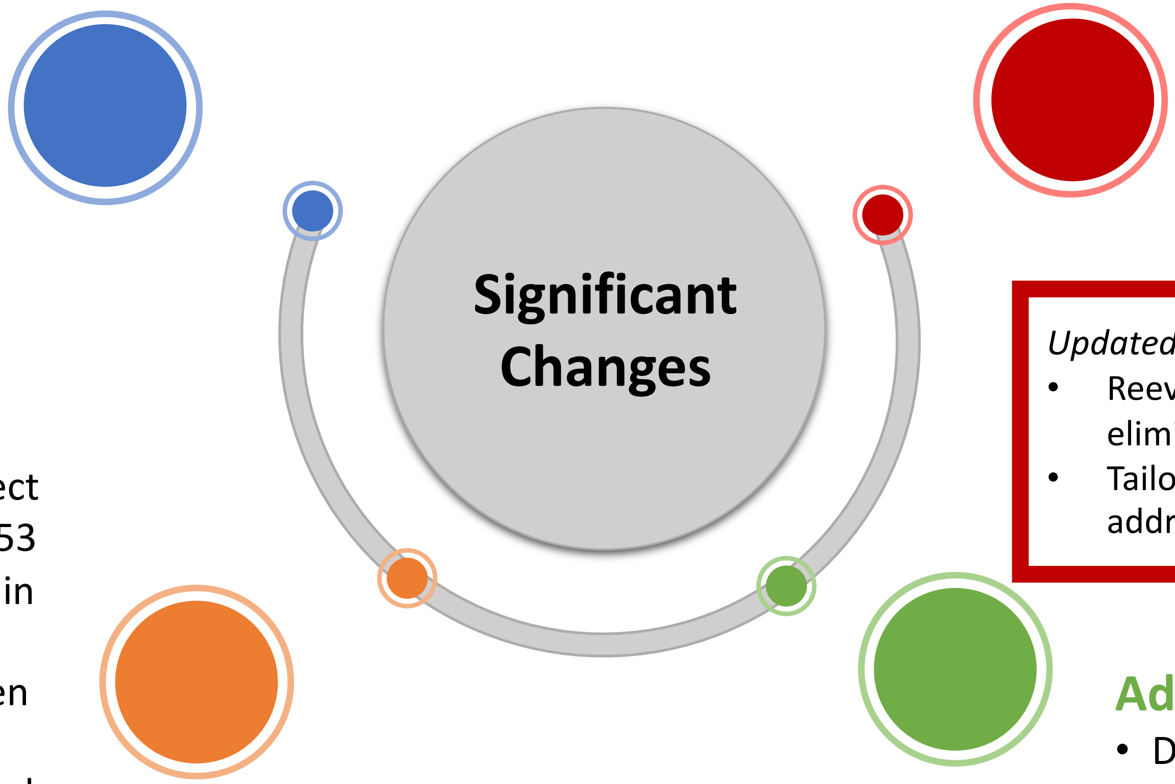
Overview: Final Public Draft SP 800-171 Rev 3

Improved Readability

Streamlined "Introduction" and "The Fundamentals" sections

Updated Security Requirements

- Added, deleted, or changed security requirements to reflect controls & families in SP 800-53 Rev 5 and moderate baseline in 800-53B
- Eliminated distinction between basic & derived requirements
- Increased specificity & grouped requirements
- Introduced organization-defined parameters (ODPs)
- Removed outdated & redundant requirements



Updated in Final Public Draft

- Reduced the number of ODPs

Updated Tailoring Criteria

- Added new tailoring categories, NA and ORC
- Recategorized selected controls from SP 800-53B moderate baseline

Updated in Final Public Draft

- Reevaluated the tailoring categories/decisions to eliminate the NFO category
- Tailored out controls that may be adequately addressed by other related controls

Added Supplemental Resources

- Developed *prototype* CUI Overlay using tailored controls in SP 800-53 Rev 5
- Created transition mapping tables & analysis of changes between SP 800-171 Revision 2 and Revision 3
- Developed an FAQ

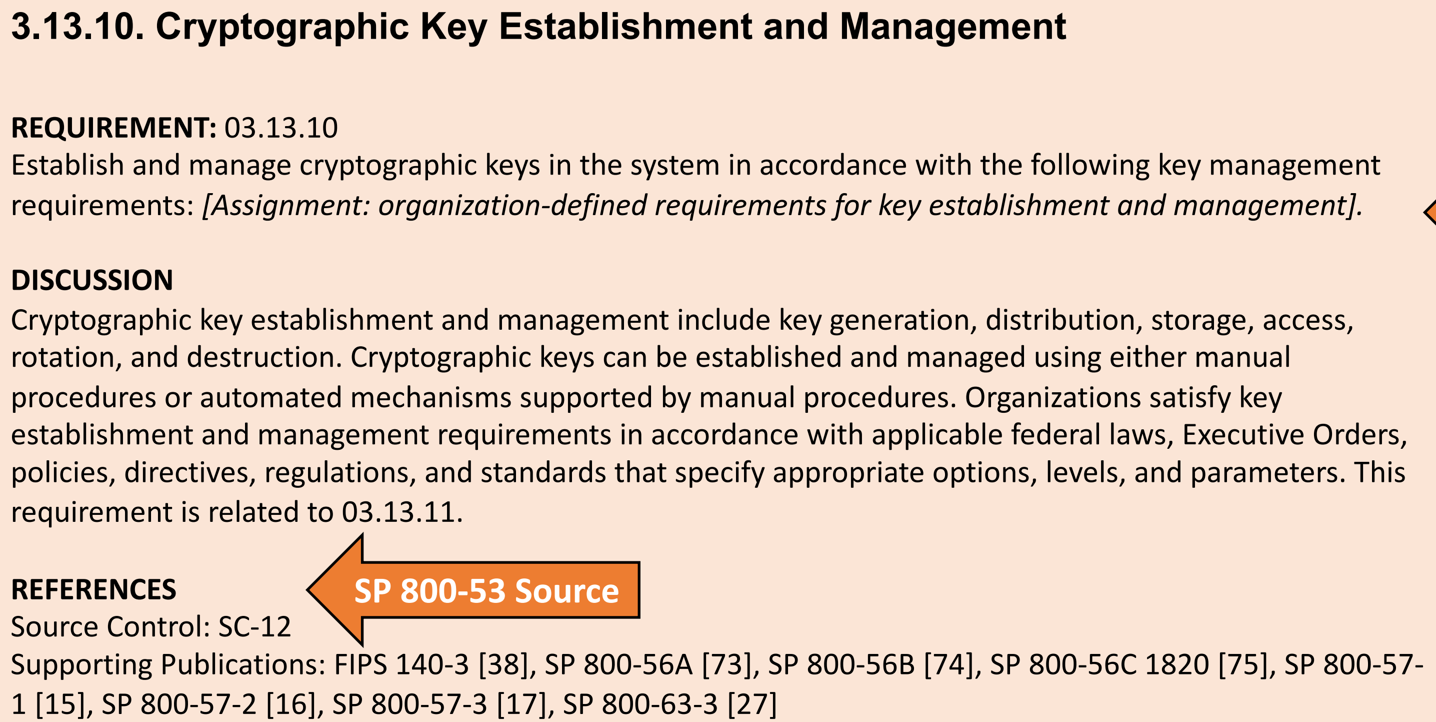
Updated Security Requirements

- ✓ Updated security requirement **structure**
- ✓ **Organization-defined parameters** (ODP) included in some requirements
  - ODPs include assignment & selection operations
- ✓ Direct link to **source** SP 800-53 controls

Updated in Final Public Draft

- Structure largely stays the same
- Included "Leading 0s" to requirements and controls

New requirement structure



3.13.10. Cryptographic Key Establishment and Management

REQUIREMENT: 03.13.10
Establish and manage cryptographic keys in the system in accordance with the following key management requirements: *[Assignment: organization-defined requirements for key establishment and management].*

DISCUSSION
Cryptographic key establishment and management include key generation, distribution, storage, access, rotation, and destruction. Cryptographic keys can be established and managed using either manual procedures or automated mechanisms supported by manual procedures. Organizations satisfy key establishment and management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards that specify appropriate options, levels, and parameters. This requirement is related to 03.13.11.

REFERENCES
Source Control: SC-12
Supporting Publications: FIPS 140-3 [38], SP 800-56A [73], SP 800-56B [74], SP 800-56C 1820 [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-63-3 [27]

New ODP

SP 800-53 Source

Updated Tailoring Criteria

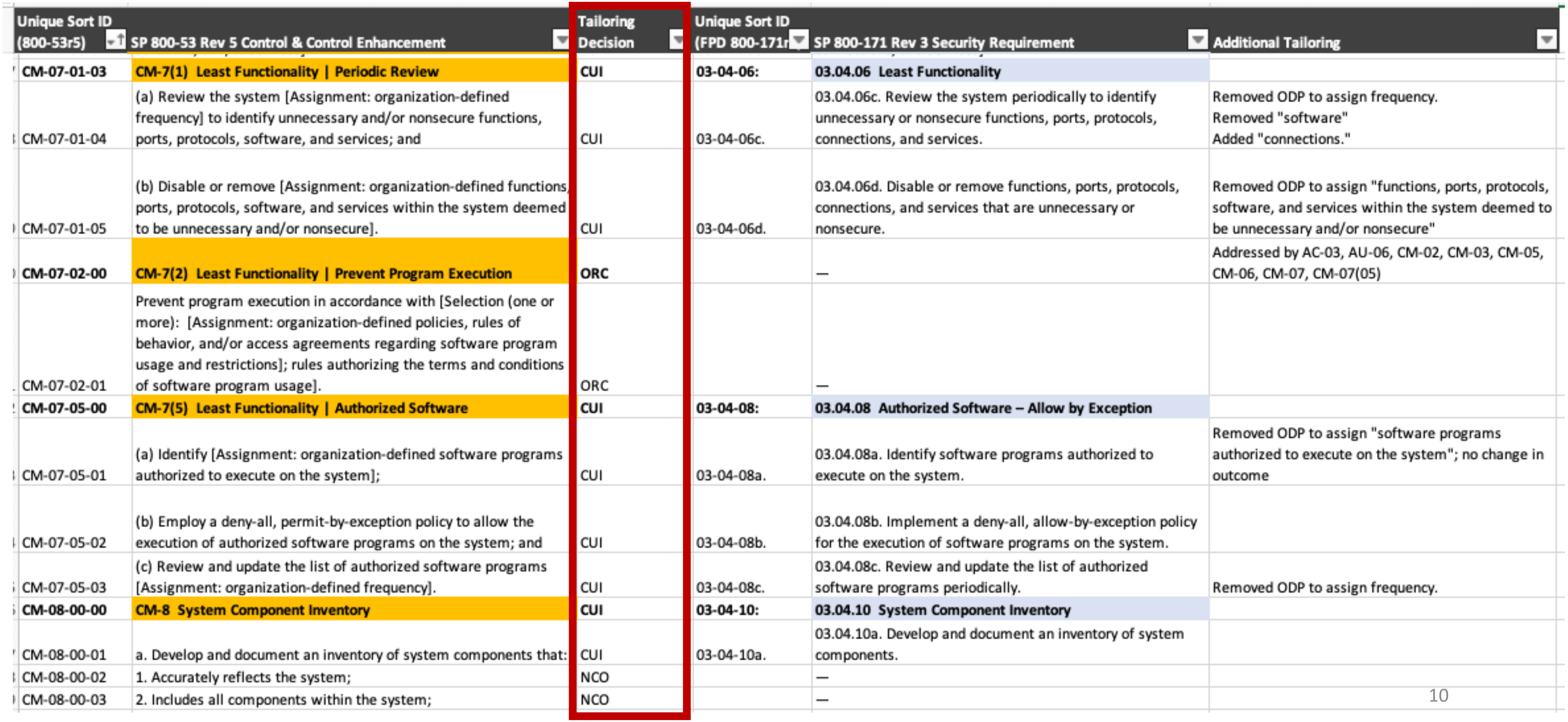
Tailoring Symbol	Tailoring Criteria	SP 800-53 Rev 4 Moderate Baseline → SP 800-171 Rev 2	SP 800-53 Rev 5 / 800-53B Moderate Baseline → FPD SP 800-171 Rev 3
NCO	Not directly related to protecting the confidentiality of CUI	58	96
NFO	Expected to be implemented by nonfederal organizations without specification	61	0
FED	Primarily the responsibility of the Federal Government	18	21
CUI	Directly related to protecting the confidentiality of CUI	125	151
ORC	The outcome of the control relating to the protection of confidentiality of CUI is adequately covered by other related controls.	New in FPD SP 800-171 Rev 3	19
NA	Not Applicable	New in IDP SP 800-171 Rev 3	50
[SP 800-53] Moderate Baseline Security Controls		**262**	**287**

- ✓ New tailoring categories, NA and ORC
- ✓ Recategorized selected controls from **SP 800-53B moderate baseline**

Updated in Final Public Draft

- Removed NFO tailoring criteria
- Added ORC (Addressed by "Other Related Controls") tailoring criteria
- Overall, ***fewer total*** security requirements

Updated Tailoring Criteria

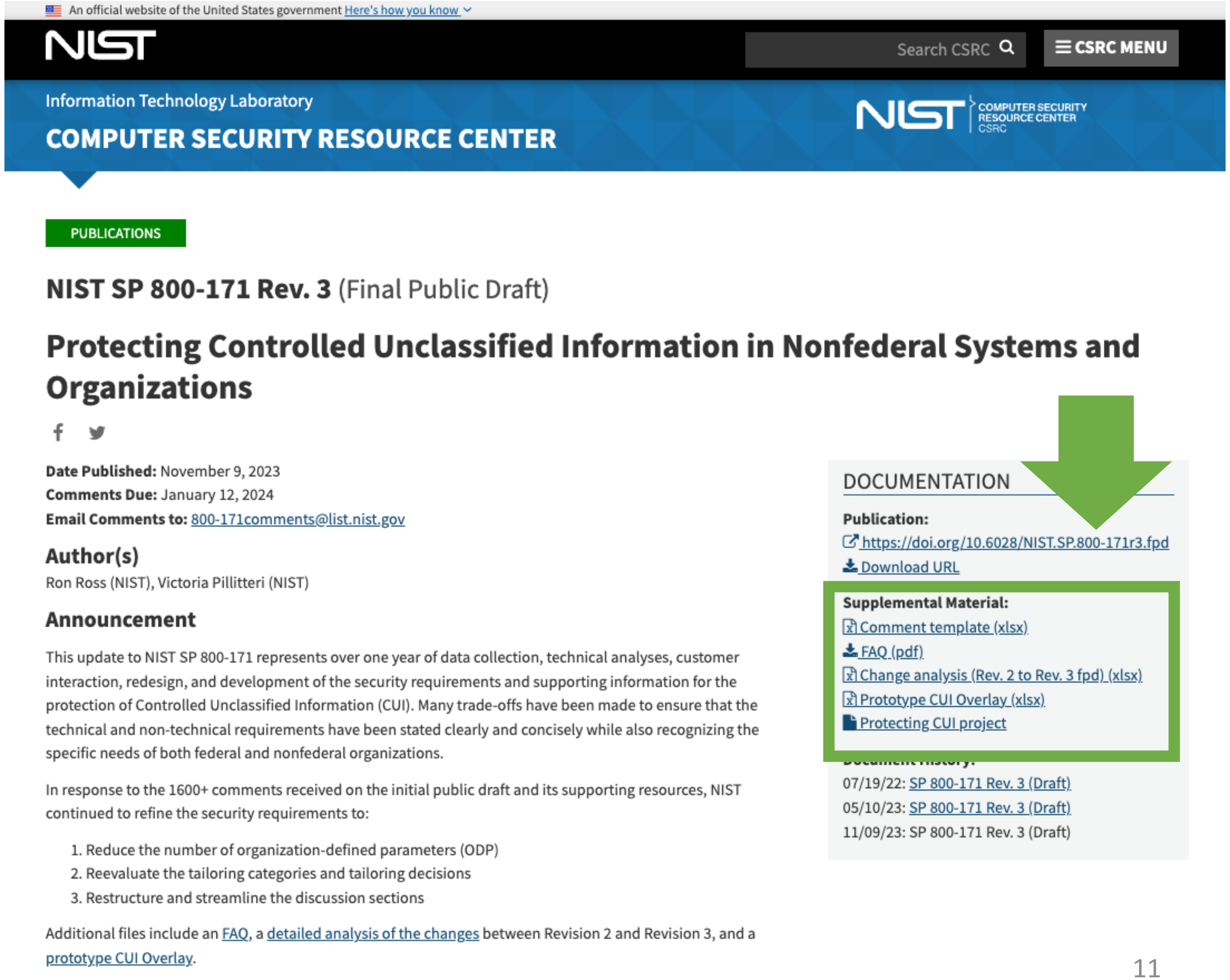


Unique Sort ID (800-53r5)	SP 800-53 Rev 5 Control & Control Enhancement	Tailoring Decision	Unique Sort ID (FPD 800-171r	SP 800-171 Rev 3 Security Requirement	Additional Tailoring
CM-07-01-03	**CM-7(1) Least Functionality | Periodic Review**	**CUI**	**03-04-06:**	**03.04.06 Least Functionality**	
CM-07-01-04	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and	CUI	03-04-06c.	03.04.06c. Review the system periodically to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.	Removed ODP to assign frequency. Removed "software" Added "connections."
CM-07-01-05	(b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].	CUI	03-04-06d.	03.04.06d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.	Removed ODP to assign "functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure"
CM-07-02-00	**CM-7(2) Least Functionality | Prevent Program Execution**	**ORC**		—	Addressed by AC-03, AU-06, CM-02, CM-03, CM-05, CM-06, CM-07, CM-07(05)
CM-07-02-01	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	ORC		—	
CM-07-05-00	**CM-7(5) Least Functionality | Authorized Software**	**CUI**	**03-04-08:**	**03.04.08 Authorized Software – Allow by Exception**	
CM-07-05-01	(a) Identify [Assignment: organization-defined software programs authorized to execute on the system];	CUI	03-04-08a.	03.04.08a. Identify software programs authorized to execute on the system.	Removed ODP to assign "software programs authorized to execute on the system"; no change in outcome
CM-07-05-02	(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and	CUI	03-04-08b.	03.04.08b. Implement a deny-all, allow-by-exception policy for the execution of software programs on the system.	
CM-07-05-03	(c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].	CUI	03-04-08c.	03.04.08c. Review and update the list of authorized software programs periodically.	Removed ODP to assign frequency.
CM-08-00-00	**CM-8 System Component Inventory**	**CUI**	**03-04-10:**	**03.04.10 System Component Inventory**	
CM-08-00-01	a. Develop and document an inventory of system components that:	CUI	03-04-10a.	03.04.10a. Develop and document an inventory of system components.	
CM-08-00-02	1. Accurately reflects the system;	NCO		—	
CM-08-00-03	2. Includes all components within the system;	NCO		—	

Added Supplemental Resources

- ✓ FAQ
- ✓ Transition Mapping Tables & Change Analysis
- ✓ Prototype CUI Overlay

https://csrc.nist.gov/pubs/sp/800/171/r3/fpd



An official website of the United States government Here's how you know

NIST

Search CSRC

☰ CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

NIST SP 800-171 Rev. 3 (Final Public Draft)

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Date Published: November 9, 2023
Comments Due: January 12, 2024
Email Comments to: 800-171comments@list.nist.gov

Author(s)

Ron Ross (NIST), Victoria Pillitteri (NIST)

Announcement

This update to NIST SP 800-171 represents over one year of data collection, technical analyses, customer interaction, redesign, and development of the security requirements and supporting information for the protection of Controlled Unclassified Information (CUI). Many trade-offs have been made to ensure that the technical and non-technical requirements have been stated clearly and concisely while also recognizing the specific needs of both federal and nonfederal organizations.

In response to the 1600+ comments received on the initial public draft and its supporting resources, NIST continued to refine the security requirements to:

1. Reduce the number of organization-defined parameters (ODP)
2. Reevaluate the tailoring categories and tailoring decisions
3. Restructure and streamline the discussion sections

Additional files include an FAQ, a detailed analysis of the changes between Revision 2 and Revision 3, and a prototype CUI Overlay.

DOCUMENTATION

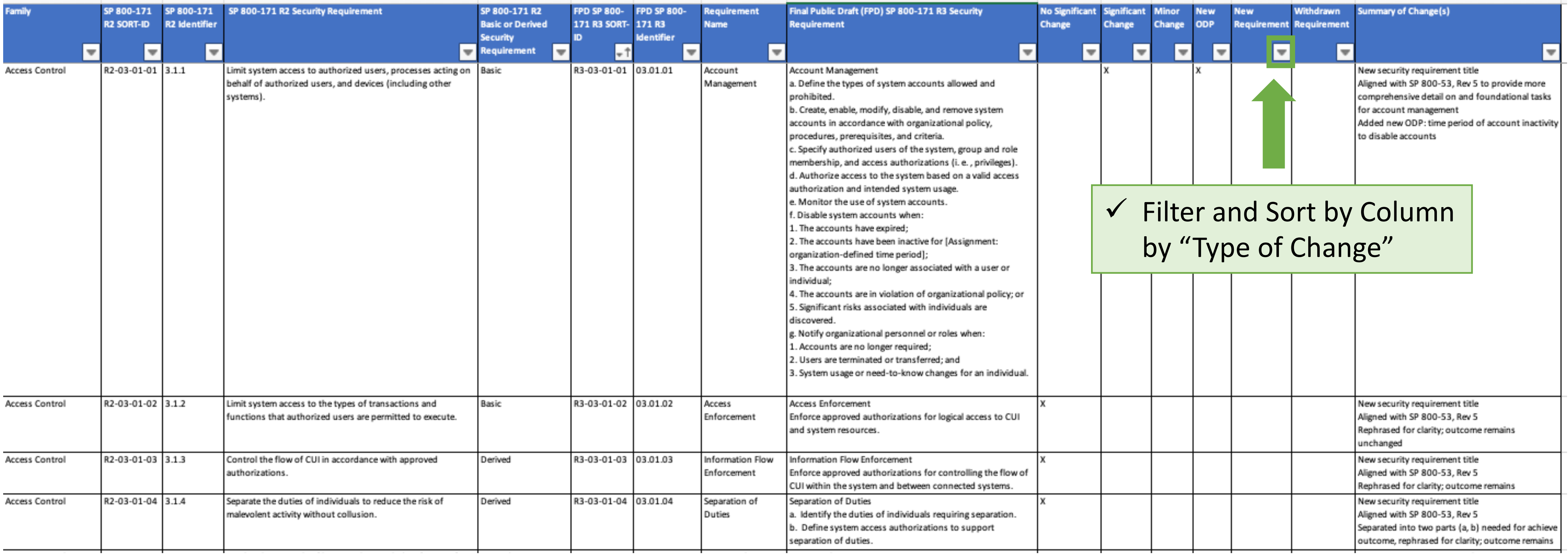
Publication:
https://doi.org/10.6028/NIST.SP.800-171r3.fpd
Download URL

Supplemental Material:
Comment template (xlsx)
FAQ (pdf)
Change analysis (Rev. 2 to Rev. 3 fpd) (xlsx)
Prototype CUI Overlay (xlsx)
Protecting CUI project

Document History:
07/19/22: SP 800-171 Rev. 3 (Draft)
05/10/23: SP 800-171 Rev. 3 (Draft)
11/09/23: SP 800-171 Rev. 3 (Draft)

Added Supplemental Resources

Change Analysis SP 800-171 Rev 2 to FPD Rev 3

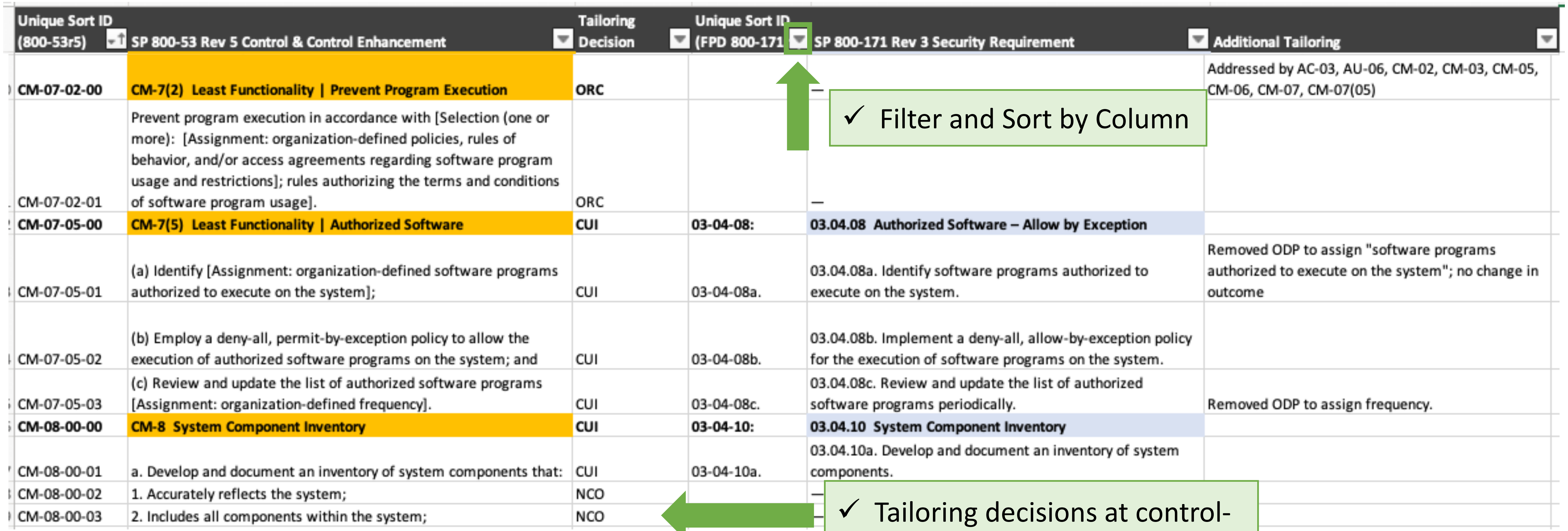


Family	SP 800-171 R2 SORT-ID	SP 800-171 R2 Identifier	SP 800-171 R2 Security Requirement	SP 800-171 R2 Basic or Derived Security Requirement	FPD SP 800-171 R3 SORT-ID	FPD SP 800-171 R3 Identifier	Requirement Name	Final Public Draft (FPD) SP 800-171 R3 Security Requirement	No Significant Change	Significant Change	Minor Change	New ODP	New Requirement	Withdrawn Requirement	Summary of Change(s)
Access Control	R2-03-01-01	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Basic	R3-03-01-01	03.01.01	Account Management	Account Management a. Define the types of system accounts allowed and prohibited. b. Create, enable, modify, disable, and remove system accounts in accordance with organizational policy, procedures, prerequisites, and criteria. c. Specify authorized users of the system, group and role membership, and access authorizations (i. e. , privileges). d. Authorize access to the system based on a valid access authorization and intended system usage. e. Monitor the use of system accounts. f. Disable system accounts when: 1. The accounts have expired; 2. The accounts have been inactive for [Assignment: organization-defined time period]; 3. The accounts are no longer associated with a user or individual; 4. The accounts are in violation of organizational policy; or 5. Significant risks associated with individuals are discovered. g. Notify organizational personnel or roles when: 1. Accounts are no longer required; 2. Users are terminated or transferred; and 3. System usage or need-to-know changes for an individual.		X		X			New security requirement title Aligned with SP 800-53, Rev 5 to provide more comprehensive detail on and foundational tasks for account management Added new ODP: time period of account inactivity to disable accounts
Access Control	R2-03-01-02	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Basic	R3-03-01-02	03.01.02	Access Enforcement	Access Enforcement Enforce approved authorizations for logical access to CUI and system resources.	X						New security requirement title Aligned with SP 800-53, Rev 5 Rephrased for clarity; outcome remains unchanged
Access Control	R2-03-01-03	3.1.3	Control the flow of CUI in accordance with approved authorizations.	Derived	R3-03-01-03	03.01.03	Information Flow Enforcement	Information Flow Enforcement Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.	X						New security requirement title Aligned with SP 800-53, Rev 5 Rephrased for clarity; outcome remains
Access Control	R2-03-01-04	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Derived	R3-03-01-04	03.01.04	Separation of Duties	Separation of Duties a. Identify the duties of individuals requiring separation. b. Define system access authorizations to support separation of duties.	X						New security requirement title Aligned with SP 800-53, Rev 5 Separated into two parts (a, b) needed for achieve outcome, rephrased for clarity; outcome remains

- ✓ Filter and Sort by Column by “Type of Change”

Added Supplemental Resources

Prototype CUI Overlay

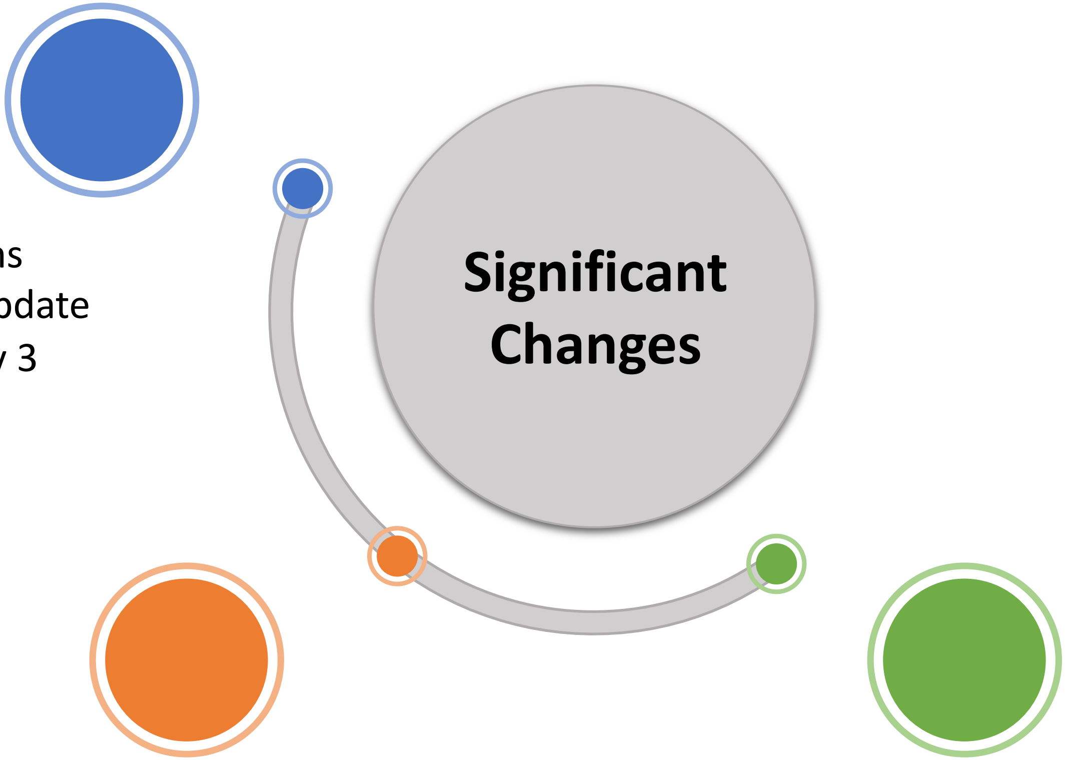


Unique Sort ID (800-53r5)	SP 800-53 Rev 5 Control & Control Enhancement	Tailoring Decision	Unique Sort ID (FPD 800-171	SP 800-171 Rev 3 Security Requirement	Additional Tailoring
CM-07-02-00	**CM-7(2) Least Functionality | Prevent Program Execution**	**ORC**		—	Addressed by AC-03, AU-06, CM-02, CM-03, CM-05, CM-06, CM-07, CM-07(05)
CM-07-02-01	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	ORC		—	
CM-07-05-00	**CM-7(5) Least Functionality | Authorized Software**	**CUI**	**03-04-08:**	**03.04.08 Authorized Software – Allow by Exception**	
CM-07-05-01	(a) Identify [Assignment: organization-defined software programs authorized to execute on the system];	CUI	03-04-08a.	03.04.08a. Identify software programs authorized to execute on the system.	Removed ODP to assign "software programs authorized to execute on the system"; no change in outcome
CM-07-05-02	(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and	CUI	03-04-08b.	03.04.08b. Implement a deny-all, allow-by-exception policy for the execution of software programs on the system.	
CM-07-05-03	(c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].	CUI	03-04-08c.	03.04.08c. Review and update the list of authorized software programs periodically.	Removed ODP to assign frequency.
CM-08-00-00	**CM-8 System Component Inventory**	**CUI**	**03-04-10:**	**03.04.10 System Component Inventory**	
CM-08-00-01	a. Develop and document an inventory of system components that:	CUI	03-04-10a.	03.04.10a. Develop and document an inventory of system components.	
CM-08-00-02	1. Accurately reflects the system;	NCO		—	
CM-08-00-03	2. Includes all components within the system;	NCO			

✓ Filter and Sort by Column

✓ Tailoring decisions at control- and requirement—item level

Overview: Initial Public Draft SP 800-171A Rev 3



Significant Changes

Improved Readability

- Updated “Introduction” and “The Fundamentals” sections
- One time version number update to align with SP 800-171 Rev 3

Updated Assessment Procedures

- Restructured assessment procedure syntax to align with NIST SP 800-53A Rev 5
- Includes ODPs (consistent with SP 800-171 security requirements)

Added Supplemental Resources

- SP 800-171A assessment procedures in spreadsheet format

Updated Assessment Procedures

SP 800-171 Rev 3 (FPD)

3.13.10. Cryptographic Key Establishment and Management

REQUIREMENT: 03.13.10
Establish and manage cryptographic keys in the system in accordance with the following key management requirements: *[Assignment: organization-defined requirements for key establishment and management]*.

DISCUSSION
Cryptographic key establishment and management include key generation, distribution, storage, access, rotation, and destruction. Cryptographic keys can be established and managed using either manual procedures or automated mechanisms supported by manual procedures. Organizations satisfy key establishment and management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards that specify appropriate options, levels, and parameters. This requirement is related to 03.13.11.

REFERENCES
Source Control: SC-12
Supporting Publications: FIPS 140-3 [38], SP 800-56A [73], SP 800-56B [74], SP 800-56C 1820 [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-63-3 [27]

3.13.10. Cryptographic Key Establishment and Management

REQUIREMENT: 03.13.10

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.10.ODP[01]: requirements for key establishment and management are defined.

A.03.13.10[01]: cryptographic keys are established in the system in accordance with the following key management requirements: <A.03.13.10.ODP[01]: requirements>.

A.03.13.10[02]: cryptographic keys are managed in the system in accordance with the following key management requirements: <A.03.13.10.ODP[01]: requirements>.

ASSESSMENT METHODS AND OBJECTS

Examine - [SELECT FROM: system and communications protection policy and procedures; procedures for cryptographic key establishment and management; system design documentation; system configuration settings; cryptographic mechanisms; system audit records; system security plan; other relevant documents or records]

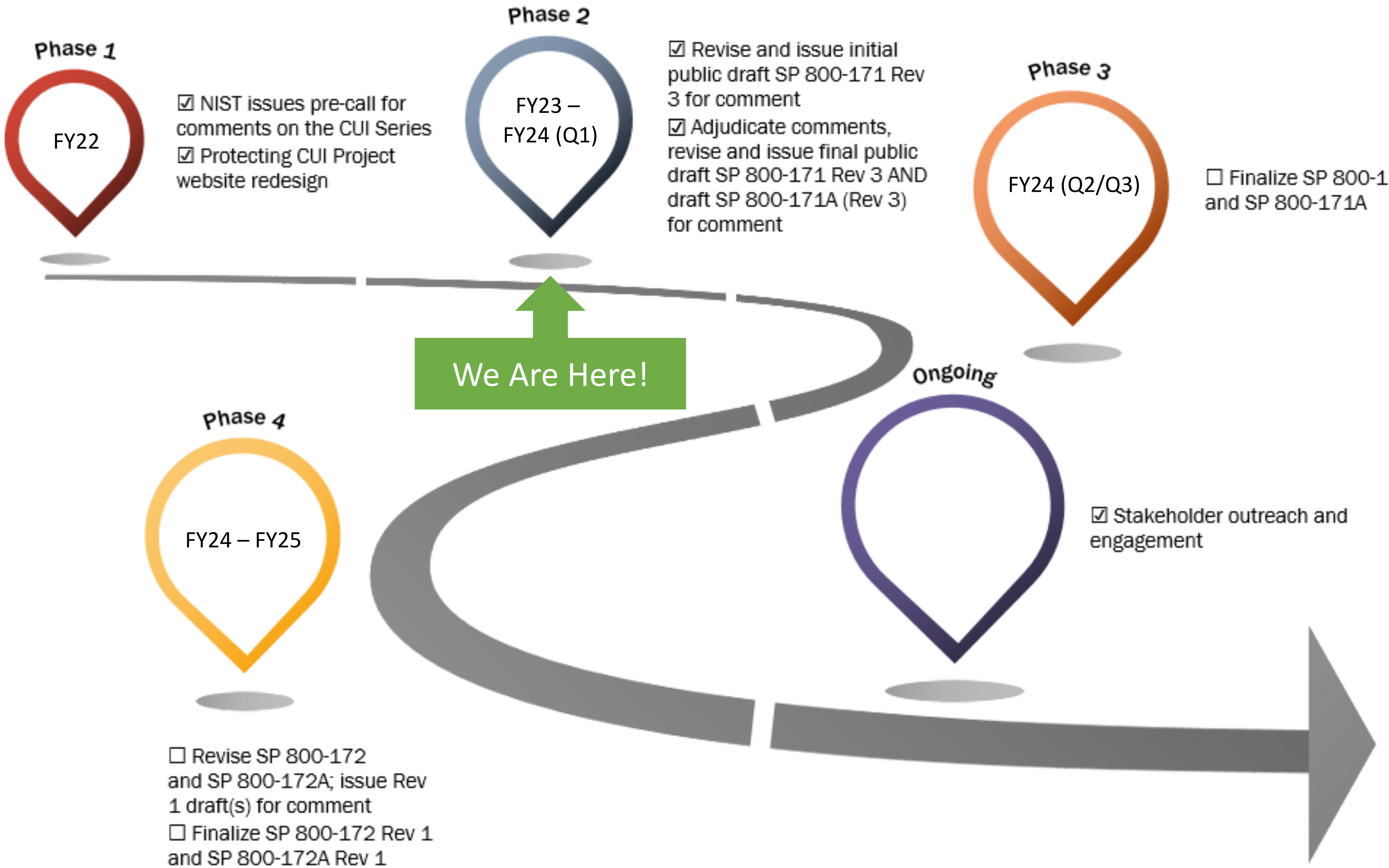
Interview - [SELECT FROM: personnel with responsibilities for cryptographic key establishment and/or management; personnel with information security responsibilities; system administrators]

Test - [SELECT FROM: mechanisms for supporting and/or implementing cryptographic key establishment and management]

REFERENCES

Source Assessment Procedure: SC-12

Looking Ahead for the CUI Series



Phase 1

FY22

☑ NIST issues pre-call for comments on the CUI Series
☑ Protecting CUI Project website redesign

Phase 2

FY23 – FY24 (Q1)

☑ Revise and issue initial public draft SP 800-171 Rev 3 for comment
☑ Adjudicate comments, revise and issue final public draft SP 800-171 Rev 3 AND draft SP 800-171A (Rev 3) for comment

We Are Here!

Phase 3

FY24 (Q2/Q3)

☐ Finalize SP 800-171 Rev 3 and SP 800-171A

Ongoing

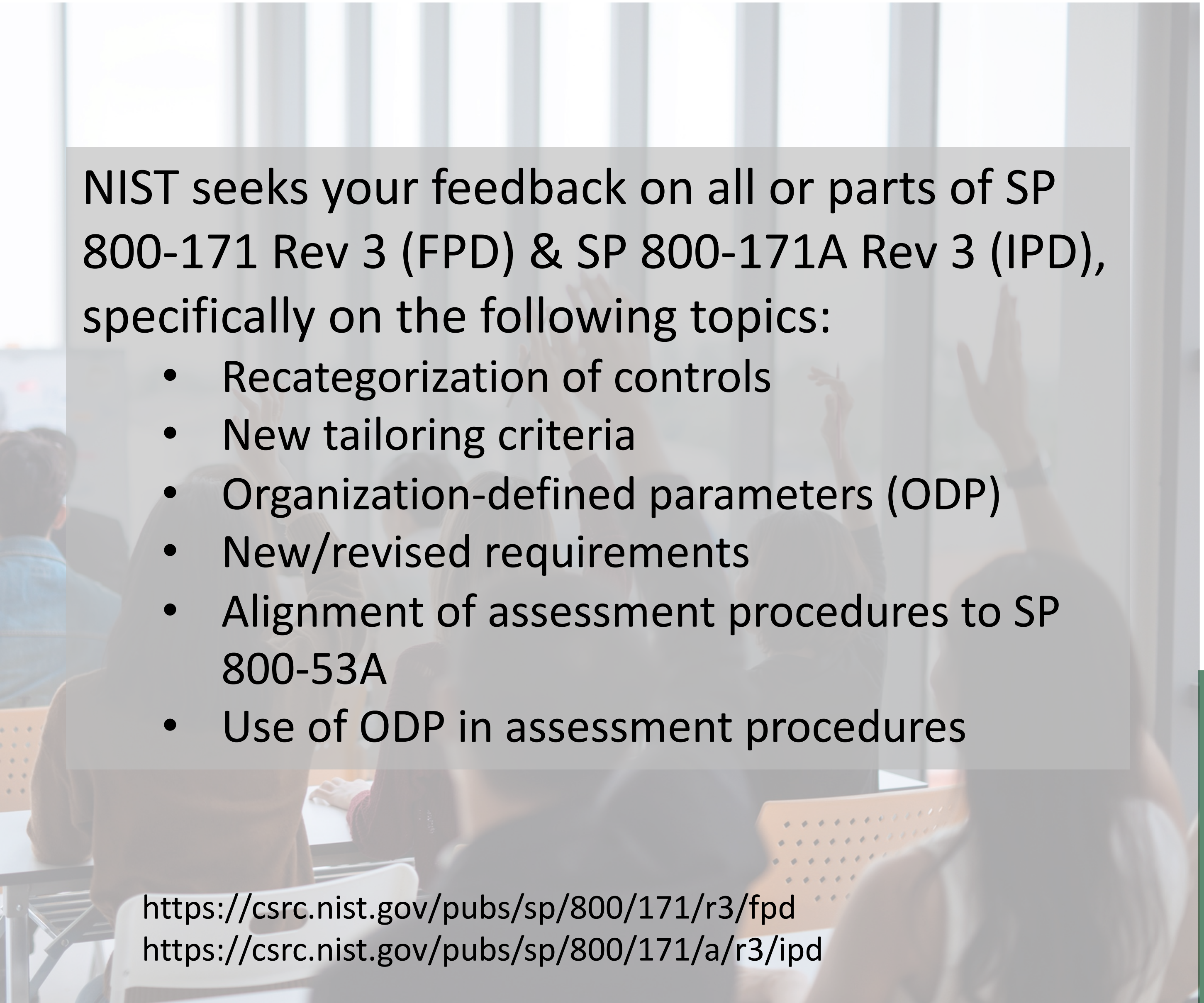
☑ Stakeholder outreach and engagement

Phase 4

FY24 – FY25

☐ Revise SP 800-172 and SP 800-172A; issue Rev 1 draft(s) for comment
☐ Finalize SP 800-172 Rev 1 and SP 800-172A Rev 1

Public Comment Period Until Jan 12, 2024



NIST seeks your feedback on all or parts of SP 800-171 Rev 3 (FPD) & SP 800-171A Rev 3 (IPD), specifically on the following topics:

- Recategorization of controls
- New tailoring criteria
- Organization-defined parameters (ODP)
- New/revised requirements
- Alignment of assessment procedures to SP 800-53A
- Use of ODP in assessment procedures

https://csrc.nist.gov/pubs/sp/800/171/r3/fpd
https://csrc.nist.gov/pubs/sp/800/171/a/r3/ipd

Submit your feedback to
800-171comments@list.nist.gov
by January ~~12~~ **26**, 2024

Comments received in response to this request will be posted on the Protecting CUI project site.

Submitters' names and affiliations (when provided) will be included, while contact information will be removed.

STAY IN TOUCH

CONTACT US

https://csrc.nist.gov/Projects/protecting-CUI

800-171comments@list.nist.gov

@NISTcyber